DEPARTMENT OF THE ARMY
WASHINGTON, DC 20310

HQDA Ltr 25-03-1

SAIS–IOA

23 April 2003

Expires 23 April 2005

SUBJECT: Transition of Information Assurance Duties and Responsibilities

SEE DISTRIBUTION

1. **Purpose.** This letter provides policy and guidance for information assurance (IA) roles and responsibilities. Information in this policy will be incorporated into the next revisions of pertinent regulations and manuals.

2. **Applicability.** This policy applies to the Active Army; the Army National Guard of the United States, including periods when operating in its Army National Guard (ARNG) capacity; the United States Army Reserve; and contractor personnel (when authorized by contract) unless otherwise stated.

3. **Proponent and exception authority.** The proponent of this letter is the Chief Information Officer, G–6 (CIO/G–6). The proponent has delegated exception authority to the Director of Information Assurance, Enterprise Systems Technology Activity (ESTA), Network Enterprise Technology Command (NETCOM) for all matters pertaining to Army networks security.

4. **References.**

a. Required publications.

(1) General Order No. 5, Establishment of U.S. Army Network Enterprise Technology Command/9th Army Signal Command; Transfer and Redesignation of the Headquarters and Headquarters Company, 9th Army Signal Command; Discontinuance of the Communications Electronic Services Office and the Information Management Support Agency, 13 August 2002.

(2) AR 25–1, Army Information Management, 31 May 2002.

(3) AR 380–19, Information Systems Security, 27 February 1998.

(4) Information Management Implementation Plan, Phase I, a publication of the Deputy Chief of Staff for Command, Control, Communications, and Computers, dated 30 November 2001. Obtain through the Army Knowledge Online portal at the Army CIO/G–6 Information Management/Information Technology Collaboration Center link.

b. Related publication. AR 380–67, Personnel Security Program, 9 September 1988.

5. Explanation of abbreviations. Abbreviations used in this letter are explained in the glossary.

6. Background. The Army began a transition to an "enterprise-level" state of operating and maintaining Army information technology (IT) with the establishment of the NETCOM on 1 October 2002. Defending the networks and Army IA will be NETCOM's core competency. The Chief of Staff, Army and the Vice Chief of Staff, Army have stated that IA is a force protection issue, that commanders are responsible for IA, and that commanders at all levels are responsible for establishing an information assurance program. To achieve IA operating and maintenance goals, there will be a period of transition between the current Army IA program (focused on the major Army command (MACOM)) and the objective of a MACOM/regionalized program. As Army begins this transition, all current and future IA managers and officers will work together to ensure that major IA responsibilities transform in an orderly manner. The scope of the IA role of the MACOMs will lessen, but MACOM commanders will still need to establish/maintain a MACOM IA program and to appoint/retain IA personnel to support the Army IA program. The scope of the program executive office (PEO) and direct reporting program manager (PM) IA programs will not change but will play a more prominent role in the objective Army enterprise solution. The Assistant Chief of Staff for Installation Management (ACSIM) and the ACSIM Installation Management Agency (IMA) and IMA regional directors will have a new IA role. At each IMA region, the regional chief information officer (RCIO) will be the IA staff proponent on the IMA director's staff. Three RCIOs will be outside continental U.S. (OCONUS) (Europe, Pacific, and Korea); four RCIOs will be CONUS (Northwest, Southwest, Northeast, and Southeast); and four RCIOs will be functional (Army National Guard, Army Reserve, Medical Command, and Corps of Engineers). The functional RCIOs are technical control (TECHCON) to the NETCOM for network operations (NETOPS), including IA.

7. IA responsibilities. The Army IA responsibility includes but is not limited to—

a. Policy implementation and oversight.

b. IA Vulnerability Alert (IAVA) dissemination/compliance reporting.

c. Training/certification of systems administrators (SAs), IA professionals, and users.

d. Certification and accreditation.

e. Information system (IS) incident reporting and handling.

f. IA resource identification and validation.

g. Communications security (COMSEC).

8. IA personnel. To ensure that the IA duties and responsibilities are executed at all levels of the Army, the Commanding General, NETCOM; commanders of MACOMs; directors of Directorates of Information Management (DOIMs); officials of PEOs; direct reporting PMs; and RCIOs will appoint IA personnel to execute specific duties and responsibilities (see para 11).

9. Mission scope. The scope of the IA mission is as follows and will evolve during this period of transition:

a. MACOMs. The scope of the MACOM IA program includes the appointment of tenant IA managers (IAM) and IA security officers (IASOs) that support the installation IAMs and RCIOs. The MACOMs also will coordinate with the RCIO information assurance program manager (IAPM) to ensure that the tenant IAMs and IASOs are executing their IA duties and responsibilities.

b. DOIMs. Each director of information management (DOIM) is responsible for IA at the installation level. The DOIM will appoint the installation IAM. The Installation IAM will be assigned to the DOIM.

c. PEOs and direct reporting PMs. The scope of the PEO and direct reporting PM IA responsibility includes unique systems of the PEO and direct reporting PM. In some cases the PEO and direct reporting PM own and operate the IS, making the IS clearly the responsibility of the PEO/direct reporting PM. In some instances the PEO and direct reporting PM maintain the configuration baseline for a system and are therefore responsible for developing and disseminating timely Field Engineering Notes (FENs)/ Engineering Change Proposals (ECPs) but do not own or operate the system. In this instance, the PEO and direct reporting IAPM must work closely with the RCIOs to ensure that the system administrators are entered into the Compliance Reporting Database (CRD) and that the appropriate installation IAM and RCIO IAPM has visibility over the application of the FEN/ECP.

d. NETCOM/RCIOs. The scope of the RCIO IA responsibilities includes all common user ISs that are not unique to the MACOM, PEO, or direct reporting PM. It also includes visibility of all ISs in the region regardless of who owns and operates an IS. NETCOM will organize the visibility of all ISs on an installation and regional basis as the CRD matures.

10. Establishment of information assurance programs. Each of the following officials will establish an information assurance program and appoint an IA program manager (IAPM) to manage the program and serve as the IA representative of the respective commander, director, or activity head:

a. Administrative Assistant to the Secretary of the Army (serving as the commander of the Headquarters, Department of the Army MACOM).

b. Chief, National Guard Bureau (CNGB).

c. Chief, Army Reserve (CAR).

d. Commanders, MACOMs.

e. Commander, U.S. Army Community and Family Support Center (USACFSC).

f. Activity head, PEO.

g. Direct reporting PMs.

h. Regional chief information officers.

11. Responsibilities.

a. The information assurance program manager. The IAPM will be accountable for establishing and assessing the effectiveness of the IA program within his or her organization. U.S. Government personnel (military or civil servant) will normally fill the IAPM position. When this is not possible, a U.S. contractor may temporarily (until Government personnel can be appointed) fill this position. Requests to appoint a U.S. contractor for a specified period of time will be sent to Headquarters, Department of the Army (HQDA) CIO/G–6 for approval. The IAPM must be a U.S. citizen and hold a U.S. Government security clearance commensurate with the level of information the organization processes. This function is considered a critical-sensitive automatic data processing (ADP) position and is designated as ADP–I per Army Regulation (AR) 380–67, appendix K. The IAPM must be IA trained/certified and maintain the certification in accordance with CIO/G–6 guidance. The IAPM will—

(1) Ensure appointment of the appropriate number of IA personnel (alternate IAPM, information assurance network manager (IANM), information assurance network officer (IANO), IAM, and tenant IAM and IASO) necessary to execute IA duties and responsibilities. On 1 October 2002, the Army began a transition of the responsibility for the management of installations from MACOMs to the ACSIM. Each installation will consist of tenants that may belong to more than one MACOM, PEO or direct reporting PM. IAPMs of organizations that have tenants on an installation will need to ensure that tenant IAMs and IASOs are appointed. These IAMs and IASOs will support the installation IAM and the applicable RCIO, executing IA duties in support of common user IS. The IAPM of the organization that installation tenants are assigned to must coordinate closely with the installation IAM and RCIO IAPM to ensure that tenant IAMs and IASOs are assigned and executing their IA duties and responsibilities.

(2) Promulgate HQDA IA guidance and develop implementing IA guidance within their organization that is necessary to support the scope of their duties and responsibilities.

(3) Establish and provide oversight for an IA vulnerability process to ensure the dissemination, application, and reporting of IAVAs, Information Assurance Bulletins (IABs), and Information Assurance Technical Tips (IATTs).

(4) Develop a process for entering compliance data into the Army CRD for applicable IS. The PEO and direct reporting PM IAPMs must work closely with the Installation IAMs and RCIO IAPMs to ensure visibility of PEO/direct reporting PM systems that are on that installation and in that region.

(5) Establish a process to ensure that all IS incident reporting is accomplished in accordance with HQDA guidance.

(6) Establish a process to ensure and document the status of all IS certification and accreditation in accordance with the Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP).

(7) Provide oversight for an IA training program that includes but is not limited to IA training for IA personnel, system administrators, and designated accreditation authorities and awareness training for users.

(8) Identify and validate IA resource requirements to NETCOM in accordance with HQDA guidance.

(9) Establish management controls for applicable IS.

(10) The RCIO IAPM will ensure the appointment of an installation IAM for each installation or cluster of small post/camps/stations within the region.

b. Information assurance network manager. The CAR; CNGB; Commander, USACFSC; MACOM commanders; PEO head; direct reporting PMs; RCIOs; and the Administrative Assistant to the Secretary of the Army (acting as the HQDA MACOM commander) will appoint the number of IANMs necessary to adequately execute the IANM duties and responsibilities. The MACOM/PEO/direct reporting PM/RCIO IANM may serve as the alternate IAPM. U.S. Government personnel (military or civil servant) will normally fill the IANM position. When this is not possible, a U.S. contractor may temporarily (until Government personnel can be appointed) fill this position. Submit a request to appoint a U.S. contractor for a specified period of time to HQDA CIO/G–6 for approval. The IANM must be a U.S. citizen and hold a U.S. Government security clearance/access approval commensurate with the level of information the organization processes. Designate this function ADP–I. The IANM must be IA certified and maintain the certification in accordance with HQDA (CIO/G–6) guidance. The IANM will—

(1) Provide technical assistance and support to the IAPM.

(2) Ensure that the hardware and software components of the network infrastructure

are properly configured and that the security features and controls appropriate to the intended level of system operation are properly set.

(3) Assist the IAPM in providing technical oversight, implementation, and reporting of IAVA/IABs/IATTs.

(4) Provide oversight for the periodic use of authorized IA tools to scan for vulnerabilities.

c. Information assurance network officer. The IANM will ensure that an appropriate number of IANOs are appointed that are necessary to execute the IANO duties and responsibilities in accordance with CIO/G–6 guidance. Designate the MACOM/PEO/direct reporting PM unique IANO position ADP–I or –II as appropriate, in accordance with appendix K, AR 380–67. The IANO must be IA certified and maintain the certification in accordance with CIO/G–6 guidance. The IANO will—

(1) Provide technical assistance and support to the IANM.

(2) Assist the IANM to ensure that the hardware and software components of the network infrastructure are properly configured and that the security features and controls appropriate to the intended level of system operation are properly set.

(3) Assist the IANM in providing oversight to ensure proper implementation, application, and reporting of IAVAs/IABs/IATTs.

(4) Assist the IANM to provide oversight for the periodic use of authorized IA tools to scan for vulnerabilities.

d. Information assurance manager. The information assurance manager (IAM) will hold a U.S. Government security clearance/access approval commensurate with the level of information processed. Designate this position ADP–I, ADP–II, or ADP–III, as appropriate, in accordance with AR 380–67, appendix K. The IAM must be IA certified, and maintain the certification in accordance with CIO/G–6 guidance. The IAM will—

(1) Ensure the appointment of the appropriate number of IASO personnel necessary to execute IASO IA duties and responsibilities.

(2) Disseminate and provide oversight for the implementation of IA policy and guidance.

(3) Assist the IANM to ensure that Information Assurance Vulnerability Alerts (IAVA), IA Bulletins, and IA Technical Tips are disseminated to systems administrators within their areas of responsibility.

(4) Gather the documentation for the IAPM that is necessary for input and routine updating in the Army CRD.

(5) Report all IS incidents in accordance with IAPM guidance.

(6) Ensure that all IS within their scope of responsibility is properly certified and accredited in accordance with the DITSCAP and provide the information to the IAPM.

(7) Ensure that training requirements and training/certification status of system administrators, IA personnel, IA awareness training for users are provided to the IAPM.

(8) Assist the IAPM in the identification and validation of IA resource requirements.

(9) Provide input to the IAPM for management controls.

(10) The installation IAM will be responsible for managing all the IAMs on an installation or cluster of small post/camps/stations.

(11) Tenant IAMs will report to/assist the installation IAM.

(12) Installation IAMs will report to the RCIO IAPM.

e. Information assurance security officer. The IAM will ensure that an IASO is assigned for each IS or group of ISs. The IASO position will be designated ADP–I, ADP–II, or ADP–III in accordance with AR 380–67, appendix K. The IASO must be IA certified and maintain the certification. PEOs and direct reporting PMs will appoint a pre-deployment IASO for each developmental system. The IASO will—

(1) Disseminate and ensure implementation of IA policy and guidance.

(2) Assist the IAM to ensure that Information Assurance Vulnerability Alerts (IAVA), IA Bulletins, and IA Technical Tips are disseminated to appropriate personnel within their area of responsibility.

(3) Assist the IAM in obtaining and in-putting information necessary for input and routine updating in the Army CRD.

(4) Ensure that all IS incidents that occur within their area of responsibility are reported to the appropriate IAM.

(5) Ensure that all IS within their scope of responsibility is properly certified and accredited in accordance with the DITSCAP and provide the information to the appropriate IAM.

(6) Ensure that the requirements and status of training, including IA awareness training, of system administrators and IA personnel is provided to the appropriate IAM.

(7) Assist the IAM in the identification and validation of IA resource requirements.

(8) Provide input to the IAM for management evaluation controls.

(9) Tenant IASOs will report to tenant IAM.

12. Summary of major duties and responsibilities.

a. Policy implementation and oversight. The MACOMs, PEOs, and direct reporting PMs will develop and disseminate organizational procedures to implement HQDA policy for IS that are unique to the MACOM and or managed via the PEO/direct reporting PM. The Installation Management Agency, through NETCOM and the RCIOs, will develop and disseminate regional procedures to implement HQDA IA policy. The RCIO will disseminate to and depend upon the tenant appointed IAMs and IASOs to implement IA policy. Although the RCIO is responsible to ensure tenants are adhering to IA policy and executing their duties and responsibilities, the MACOM and PEO/direct reporting PM will also have a key role in ensuring that tenant organizations are supporting the installation IAMs and the RCIO.

b. Information assurance vulnerability process. MACOMs, PEOs, direct reporting PMs, and RCIOs are responsible for disseminating IAVAs, IABs, and IATTs and reporting compliance in accordance with HQDA policy. As the transition to an IT enterprise management infostructure begins, the compliance and reporting requirements will remain as they are currently organized. Commanders at all levels are responsible for IAVA compliance. The IAVA compliance reporting will be done via the IAVA CRD located at Uniform Resource Locator (URL) https://informationassurance.us.army.mil. The end state of the CRD is that the MACOM will have a read-only view of their tenants on all installations. The RCIO will have visibility of the reporting via each installation in their region. The reporting and compliance data will be reported to HQDA through the RCIO chain of command. If a tenant on an installation does not comply with a directed IAVA, it is the responsibility of the RCIO and the MACOM/PEO/direct reporting PM to work together to resolve the issue and ensure compliance. This process will allow the RCIO to exercise technical control of the common user networks in their region and also allow the MACOM/PEO/direct reporting PM to have visibility of units compliance status since commanders at all levels are responsible for IAVA compliance. The Army Computer Emergency Response

Team (ACERT) and the Army Network Operations and Security Center (ANOSC) will work together to develop and disseminate the IAVAs/IABs/IATTs via the ACERT list server and the ANOSC technical tasking chain. In January 2003, NETCOM began a transformation of one CONUS RCIO at a time to reflect the new reporting/visibility responsibilities.

c. Training. System administrators (SAs) and IA personnel are required to receive specific training and certification. The MACOMs, PEOs, direct reporting PMs, and RCIOs are responsible for ensuring that SAs and IA personnel that are their responsibility are trained in accordance with HQDA policy. The MACOMs, PEOs, and direct reporting PMs will continue to identify and ensure SAs and IA personnel that are their responsibility are listed with their training status in the CRD located at URL https://informationassurance.us.army.mil. MACOMs, PEOs, and direct reporting PMs are responsible for training SAs and IA personnel that support the organizational headquarters and unique IS systems that are owned and operated by the MACOM, PEO, and direct reporting PM. The RCIOs are responsible for ensuring that SAs and IA personnel that are their responsibility are listed along with their training status in the CRD located at URL https://informationassurance.us.army.mil. The RCIOs are responsible for SAs and IA personnel who are not assigned to a MACOM, PEO or direct reporting PM owned and operated IS, to include the installation and tenant IAMs. NETCOM will start coordinating Army quarterly IA workshops, IA mobile training teams, and the location/allocation of funding for SA training sites with the RCIOs.

d. Certification and accreditation. NETCOM has overall responsibility for ensuring that all ISs are properly certified and accredited in accordance with the DITSCAP process. MACOMs, PEOs, and direct reporting PMs will be responsible for certification and accreditation of MACOM, PEO, and direct reporting PM unique systems that they own and operate. Tenant IAMs are responsible for ensuring that tenant IS are certified and accredited for that tenant organization. The tenant on an installation will provide its accreditation and certification to the installation IAM who will use it to develop the installation certification and accreditation. The RCIO will use the installation accreditation and certification to develop the regional accreditation and certification for submission to NETCOM. NETCOM is establishing a Net-worthiness process that will establish criteria for authority to connect and authority to operate. One of the criteria for authority to connect and operate is a certification and accreditation in accordance with the DITSCAP.

e. Designated approving authority. The CIO/G–6 is the designated approving authority for Army systems and networks. The Commanding General, NETCOM has been delegated the designated approving authority for the Army Enterprise. The Commanding General, NETCOM may further delegate, in writing, accreditation authority to the IMA Regional Directors. The IMA Regional Directors may further delegate, in writing, accreditation authority to the garrison commander. The garrison commander is the accreditation authority for the garrison systems and networks. Those wishing to connect to the garrison systems and/or networks must obtain approval to connect (ATC) from the designated approving authority of that garrison system and/or network. When garrison systems and/or networks require NIPRNet or SIPRNet connectivity, the garrison commander, as the designated approving authority, must request ATC from the Defense Information Systems Agency (DISA). The PEO official and MACOM commanders are the designated approving authorities for their enterprise systems and/or networks with concurrence from the Commanding General, NETCOM.

f. IA resource identification and validation. During this IA transition, resource requirements will need to be identified, validated, and documented during the program objective memorandum (POM) process, and finite IA resources that are aligned with the mission will be ensured. The Information Assurance Directorate of the Enterprise System Technology Activity of NETCOM will manage the MS4X and MX5T Management Decision Package (MDEP). The MDEP MS4X and MX5T validation processes will incorporate the CONUS RCIOs.

g. COMSEC. The Communications Security Logistics Activity (CSLA) is resourced to provide inspectors for COMSEC accounts. The CSLA missions and assets, which are currently being adjusted, will also inspect key elements of the Public Key Infrastructure (PKI). COMSEC is the cornerstone for the confidentiality of information. Commanders and IA personnel will work closely together to ensure that COMSEC continues to receive adequate oversight during this transition.

Glossary

ADP
automatic data processing

ACSIM
Assistant Chief of Staff for Installation Management

ATC
approval to connect

CONUS
continental United States

CAR
Chief, Army Reserve

COMSEC
communications security

CRD
Compliance Reporting Database

CSLA
Communications Security Logistics Activity

DISA
Defense Information Systems Agency

DITSCAP
Department of Defense Information Technology Security Certification and Accreditation Process

DOIM
Directorate of Information Management

ECP
Engineering Change Proposal

ESTA
Enterprise Systems Technology Activity

FEN
Field Engineering Notes

HQDA
Headquarters, Department of the Army

IA
information assurance

IAB
Information Assurance Bulletins

IAM
information assurance manager

IANM
information assurance network manager

IANO
information assurance network officer

IAPM
information assurance program manager

IASO
information assurance officer

IATT
Information Assurance Technical Tips

IAVA
Information Assurance Vulnerability Alerts

IMA
Installation Management Agency

IS
information system

IT
information technology

MACOM
major Army command

MDEP
management decision package

NGB
National Guard Bureau

NETCOM
Network Enterprise Technology Command

NETOPS
network operations

OCONUS
outside continental United States

PEO
program executive office

PKI
Public Key Infrastructure

PM
program manager

POM
program objective memorandum

RCIO
regional chief information officer

SA
system administrator

TECHCON
technical control

URL
Uniform Resource Locator

USACFSC
U.S. Army Community and Family Support Center

VCSA
Vice Chief of Staff

By Order of the Secretary of the Army:

ERIC K. SHINSEKI
General, United States Army
Chief of Staff

Official:

Joel B. Hudson

JOEL B. HUDSON
Administrative Assistant to the
Secretary of the Army

Distribution:

This publication is available in electronic media only and is intended for the following addresses:

HQDA (SASA) (IAPM/DCSIM/CIO)
HQDA (DACS–ZA) (IAPM/DCSIM/CIO)
HQDA (DACS–ZB) (IAPM/DCSIM/CIO)
HQDA (DACS–ZD) (IAPM/DCSIM/CIO)
HQDA (DACS–SAUS–OR) (IAPM/DCSIM/CIO)
HQDA (SACW) (IAPM/DCSIM/CIO)
HQDA (SAFM–AOA) (IAPM/DCSIM/CIO)
HQDA (SAILE) (IAPM/DCSIM/CIO)
HQDA (SAMR) (IAPM/DCSIM/CIO)
HQDA (SAALT) (IAPM/DCSIM/CIO)
HQDA (SAGC) (IAPM/DCSIM/CIO)
HQDA (SAAA–PP) (IAPM/DCSIM/CIO)
HQDA (SAIS–ZA) (IAPM/DCSIM/CIO)
HQDA (SAIG–ZA) (IAPM/DCSIM/CIO)
HQDA (SAAG–ZA) (IAPM/DCSIM/CIO)
HQDA (SALL) (IAPM/DCSIM/CIO)
HQDA (SAPA) (IAPM/DCSIM/CIO)
HQDA (SADBU) (IAPM/DCSIM/CIO)
HQDA (DAMI–ZA) (IAPM/DCSIM/CIO)
HQDA (DALO–ZA) (IAPM/DCSIM/CIO)
HQDA (DAMO–ZA) (IAPM/DCSIM/CIO)
HQDA (DAPE–ZA) (IAPM/DCSIM/CIO)
HQDA (DAEN–ZA) (IAPM/DCSIM/CIO)
HQDA (DASG–ZA) (IAPM/DCSIM/CIO)
HQDA (NGB–ZA) (IAPM/DCSIM/CIO)
HQDA (DAAR–ZA) (IAPM/DCSIM/CIO)
HQDA (DAJA–ZA) (IAPM/DCSIM/CIO)
HQDA (DACH–ZA) (IAPM/DCSIM/CIO)
HQDA (DAIM–ZA) (IAPM/DCSIM/CIO)
HQDA (JDIM–RM) (IAPM/DCSIM/CIO)

COMMANDING GENERAL
U.S. ARMY, EUROPE AND SEVENTH ARMY (IAPM/DCSIM/CIO)
COMMANDERS
EIGHTH U.S. ARMY (IAPM/DCSIM/CIO)
U.S. ARMY FORCES COMMAND (IAPM/DCSIM/CIO)
U.S. ARMY MATERIEL COMMAND (IAPM/DCSIM/CIO)
U.S. ARMY TRAINING AND DOCTRINE COMMAND (IAPM/DCSIM/CIO)
U.S. ARMY CORPS OF ENGINEERS (IAPM/DCSIM/CIO)
U.S. SPECIAL OPERATIONS COMMAND (IAPM/DCSIM/CIO)
U.S. ARMY PACIFIC (IAPM/DCSIM/CIO)
MILITARY TRAFFIC MANAGEMENT COMMAND (IAPM/DCSIM/CIO)
U.S. ARMY CRIMINAL INVESTIGATION COMMAND (IAPM/DCSIM/CIO)
U.S. ARMY MEDICAL COMMAND (IAPM/DCSIM/CIO)
U.S. ARMY INTELLIGENCE AND SECURITY COMMAND (IAPM/DCSIM/CIO)
U.S. ARMY MILITARY DISTRICT OF WASHINGTON (IAPM/DCSIM/CIO)
U.S. ARMY SOUTH (IAPM/DCSIM/CIO)

CF:
U.S. ARMY RECRUITING COMMAND (IAPM/DCSIM/CIO)
U.S. ARMY COMMUNITY AND FAMILY SUPPORT CENTER (IAPM/DCSIM/CIO)
PROGRAM EXECUTIVE OFFICER AIR AND MISSILE DEFENSE (IAPM/DCSIM/CIO)
PROGRAM EXECUTIVE OFFICE AMMUNITION (IAPM/DCSIM/CIO)
PROGRAM EXECUTIVE OFFICER AVIATION (IAPM/DCSIM/CIO)
PROGRAM EXECUTIVE OFFICER CHEMICAL AND BIOLOGICAL DEFENSE (IAPM/DCSIM/CIO)
PROGRAM EXECUTIVE OFFICER COMBAT SERVICE AND COMBAT SERVICE SYSTEM (PEO CS&CSS) (IAPM/DCSIM/CIO)
PROGRAM EXECUTIVE OFFICER COMMAND AND CONTROL AND COMMUNICATIONS TACTICAL (IAPM/DCSIM/CIO)
PROGRAM EXECUTIVE OFFICER ENTERPRISE INFORMATION SYSTEMS (IAPM/DCSIM/CIO)
PROGRAM EXECUTIVE OFFICER GROUND COMBAT SYSTEMS (IAPM/DCSIM/CIO)
PROGRAM EXECUTIVE OFFICER INTELLIGENCE ELECTRONIC WARFARE AND SENSORS (IAPM/DCSIM/CIO)
PROGRAM EXECUTIVE OFFICER SOLDIER SYSTEMS (IAPM/DCSIM/CIO)
PROGRAM EXECUTIVE OFFICER SMART MUNITIONS (IAPM/DCSIM/CIO)
PROGRAM EXECUTIVE OFFICER TACTICAL MISSILES (IAPM/DCSIM/CIO)

NW REGIONAL CIO
NE REGIONAL CIO
SW REGIONAL CIO
SE REGIONAL CIO
PACIFIC REGIONAL CIO
EUROPE REGIONAL CIO
KOREA REGIONAL CIO